Notice of Allowability	Application No.	Applicant(s)	
	09/596,948	BERSON ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment After Final filed on 4/04/2005*.

2. ☒ The allowed claim(s) is/are *1,5-8,12-15,19-22 and 25-27*.

3. ☒ The drawings filed on *10 December 2004* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Daniel B. Curtis on 4/11/2005. The application has been amended as follows:

Claim 1: A method for secure operation of a network device, comprising:

(a) assigning a digital certificate to a network user;

(b) receiving a command for operation of a network device and the digital certificate from the network user;

(c) utilizing a cryptographic key stored in the network device to authenticate the digital certificate of the network user;

(d) enabling operation of the network device if the digital certificate of the network user is authenticated and if the operation is permitted by a usage policy associated with the network user; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy associated with the printer, the copier or the facsimile machine is at least one of the policies:

a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was identified by the network device as being physically near the network device, a policy to

print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document;

wherein the usage policy associated with the scanner is at least one of the policies:

a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document .

Claim 8: A computer program embodied on a computer readable medium for secure operation of a network device, comprising:

(a) code segment embodied on the computer readable medium that assigns a digital certificate to a network user;

(b) code segment embodied on the computer readable medium that receives a command for operation of a network device and the digital certificate from the network user;

(c) code segment embodied on the computer readable

medium that utilizes a cryptographic key stored in the network

device to authenticate the digital certificate of the network user;

(d) code segment embodied on the computer readable medium that enables operation of the network device if the digital certificate of the network user is authenticated and if the operation is permitted by a usage policy associated with the network user; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy associated with the printer, the copier or the facsimile machine is at least one of the policies:

a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was identified by the network device as being physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated

with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document;

wherein the usage policy associated with the scanner is at least one of the policies:

a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document .

Claim 15 : A system for secure operation of a network device, comprising:

(a) logic that assigns a digital certificate to a network user; and

(b) a network device capable of receiving a command for operation thereof and the digital certificate from the network user, wherein the network device utilizes a cryptographic key to authenticate the digital certificate of the network user;

(c) wherein operation of the network device is enabled if the digital certificate of the network user is authenticated and if the

operation is permitted by usage policy associated with the network user ; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy associated with the printer, the copier or the facsimile machine is at least one of the policies:

a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was identified by the network device as being physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document;

wherein the usage policy associated with the scanner is at least one of the policies:

a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow

a document .

Claim 22: A method for secure identification of a network device, comprising:

(a) assigning a digital certificate to a network user;

(b) receiving a command for operation of a network device and the digital certificate from the network user;

(c) utilizing a cryptographic key stored in the network device to authenticate the digital certificate of the network user;

(d) enabling operation of the network device if the digital certificate of the network user is authenticated and if the operation is permitted by a usage policy associated with the network user; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy associated with the printer, the copier or the facsimile machine is at least one of the policies:

a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a

document only if the network user was identified by the network device as being physically near the network device; a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document;

wherein the usage policy associated with the scanner is at least one of the policies:

a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document .

Claim 27: A method for secure management of a network device, comprising:

(a) associating at least on of policy information and a computation protocol with a command for the network device;

(b) encrypting at least one of policy information and

computation protocols ;

(c) sending at least one of policy information and computation protocols to the network device;

(d) decrypting at least one of policy information and computation protocols;

(e) processing the command with the network device utilizing at least one of policy information and computation protocols; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy associated with the printer, the copier or the facsimile machine is at least one of the policies:

a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was identified by the network device as being physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing

function, a routing policy, and a policy to escrow a document;

wherein the usage policy associated with the scanner is at least one of the policies:

a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document .

Allowable Subject Matter

2. Claims 1, 5-8, 12-15, 19-22 and 25-27 are allowed.

3. The following is an examiner's statement of reasons for allowance:

3.1 Referring to the instant claims, Carroll discloses a secure server and method of operation for a distributed information system (see abstract and Fig.1).Carroll teaches a user terminal 18 includes an application 26, for example a browser, that is responsive to user input and connects to remote applications across a computer network 14. Keys used for encryption and authentication are managed by built-in key ring organizer 27 in the browser 26 (see Fig.1). Carroll teaches that authentication includes reliably

determining the identity of a network device contacting the secure application (see column 3, lines 19-21). Carroll teaches that the user terminal 18 (FIG. 1) contacts the organization server 66 over the computer network 14 (FIG. 1) and transmits access request and the digital certificate (see column 7, lines 55-60).

3.2 However, while Carroll teaching the use of the built-in key ring organizer 27 in the browser 26 (in Fig. 1), Carroll does not teach using a cryptographic key stored in the network device for authenticating the digital certificate of the network user. Debry teaches that the printer has a unique encryption key stored in it at manufacturing time. This key is also recorded in a database, securely controlled by a certificate authority (see abstract). This key is used for authentication of a digital certificate (see Fig.1 unit 50).

3.3 Neither Carroll nor Debry teach or suggest a network device having

" ... the usage policy associated with the printer, the copier or the facsimile machine is at least one of the policies:

a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was identified by the network device as being physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document;

wherein the usage policy associated with the scanner is at least one of the policies:

a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document ."

3.4. On view of the Examiner's amendment and the reasons presented herein claims 1, 5-8, 12-15, 19-22 and 25-27 are in condition for

allowance.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100